# Review of Bachelor's Thesis

**Student:** Křížová Hana, Mgr.
**Title:** Security and Privacy Oriented-Survey of Financial Applications Utilizing Blockchain (id 23162)
**Reviewer:** Malinka Kamil, Mgr., Ph.D., DITS FIT BUT

1. **Assignment complexity** **average assignment**
   Jedná se o analytickou diplomovou práci, která pokrývá poměrně širokou a aktuální oblast finančních aplikací nad technologií blockchain.
2. **Completeness of assignment requirements** **assignment fulfilled with minor reservations**
   Práce splnila všechny body zadání, ovšem některé pouze na základní úrovni. Nadbytečně nebo nedodělaně působí kapitola 2 týkající se historie. Kapitola 3 týkající se vysvětlení principů blockchain, smart kontrakt atd. je poměrně povrchní. Obdobně pak kapitola 5, která se věnuje již konkrétním finančním aplikacím, je spíše vyjmenovává, a popisuje co dělají, bez větší snahy přiblížit jakým způsobem fungují. Spíše než popis poskytovatele, mi přijde z pohledu vlastností podstatnější např. jaký blockchain používají. Autorka se též dopouští občasných faktických chyb, které ukazují nižší orientaci v oblastech kryptografie - např. str. 24 - nesprávné tvrzení o použití soukromého klíče asymetrické kryptografie pro potřebu šifrování obsahu peněženku. Nicméně práce dobře pokrývá relevantní oblasti. Další kapitola analyzující bezpečnostní hrozby je velmi solidně zpracována. Nicméně by bylo vhodné lépe začlenit reálný svět - přidat např. i cenu opatření nebo přehled reálných útoků. Případně i přidat bližší informace o principu ochran a proč by měly pomoci. V oblasti plateb mi zcela chybí množina aktuálních HW útoků na kryptopeněženky. Kapitola týkající se identifikace doporučených řešení vč. popisu jejich použití je velmi stručná. Posledním bodem zadání mělo být začlenění kategorizace do zadané referenční architektury. To je v celém textu jen velmi lehce nastíněno. Daná architektura pak v práci není ani představena.
3. **Length of technical report** **in usual extent**
   Práce je spíše rozsáhlejší, nicméně je to v souladu s rešeršním zaměřením této práce a absencí implementace.
4. **Presentation level of technical report** **65 p. (D)**
   Kromě již zmíněných výtek struktura práce poměrně dobře prezentuje problematiku. Srozumitelnost práce snižuje používání pojmů, které před tím nebyly vysvětleny, což pro čtenáře bez orientace v problematice může být hůře srozumitelné - např. gas v kontextu Etherea. Obdobně např. v obrázku 3.1 je použita zkratka txs bez bližšího vysvětlení kdekoliv v práci, že se jedná o transakce. V kapitole 5 chybí úvodník a vypovídající hodnota obrázků hlavně v kapitole 5 není moc vysoká.
5. **Formal aspects of technical report** **65 p. (D)**
   Typografická stránky práce je na velmi dobré úrovni. Nicméně obsahuje větší množství gramatických chyb.
6. **Literature usage** **85 p. (B)**
   Autorka citovala relevantní prameny a pracovala s nimi velmi dobře. Vyzdvihuji i velký počet referencí.
7. **Implementation results** **69 p. (D)**
   Analytická část práce je poměrně široká, a i přes mé výtky zdařilá. Asi největší námitky mám k tomu, že se práce většinou pohybuje pouze po povrchu a také, že se autorka plně zaměřuje na blockchainový svět. Nicméně v okamžiku, kdy se používají stejné metody a přístupy i v centralizovaném světě, měly by být i součástí porovnání produktů (alespoň v nějaké omezené míře). Dále se dá vytknout, že autorka občas opakuje obecně platné tvrzení. Vytknout se dají též některé technické nepřesnosti - např. je často poukazováno na zásadní problém Single point of failure, bez zohlednění toho, že se běžně používají technická řešení pro zvýšení odolnosti jako je redundance.
8. **Utilizability of results**
   Jde o práci kompilačního charakteru, kdy autorka dala do kontextu velké množství aktuálních informací. Práce pěkně shrnuje aplikační oblasti, je bohatá na reference a je použitelná pro zorientování se v dané problematice.
9. **Questions for defence**

   1. Mám problém s tím, když opakovaně o útoku říkáte, že je to zranitelnost (např. oracle attack). Vysvětlete tento nesoulad v kontextu bezpečnostní terminologie. Obdobně pak vysvětlete, jak může být privacy issue hrozbou.

2. Na str. 31 zmiňujete, že zajištění integrity dat musí být esenciální částí KYC blockchain aplikací. Není to by default zajištěno použitím blockchainu? Ten přece zpětně nejde změnit.

## 10. Total assessment

**75 p. good (C)**

Práce zpracovává širokou oblast finančních aplikací blockchainu, bohužel na úkor většího detailu a zanoření. Tím, že jde více do široka, tak občas spíše připomíná jmenný seznam problémů a řešení bez snahy o detailnější pochopení a interpretaci. Výsledky analýz jsou i přes svoji rozsáhlost korektní a dobře shrnují požadovaný bezpečnostní pohled. V práci mi chybělo alespoň základní srovnání s CeFi sektorem, protože některé parametry jsou poměrně zásadní, např. srovnání propustnosti transakcí Bitcoinu ve srovnání např. s VISA. Hodnocení pak dále snižují chyby. Naopak pozitivně hodnotím vysoké množství relevantní literatury a to, že je práce psaná v angličtině.

Práci navrhuji uznat jako bakalářskou a hodnotím ji "C".

In Brno 2 June 2021

Malinka Kamil, Mgr., Ph.D.
reviewer